

Práctica 1.1. Protocolo IPv4. Servicio DHCP

Objetivos

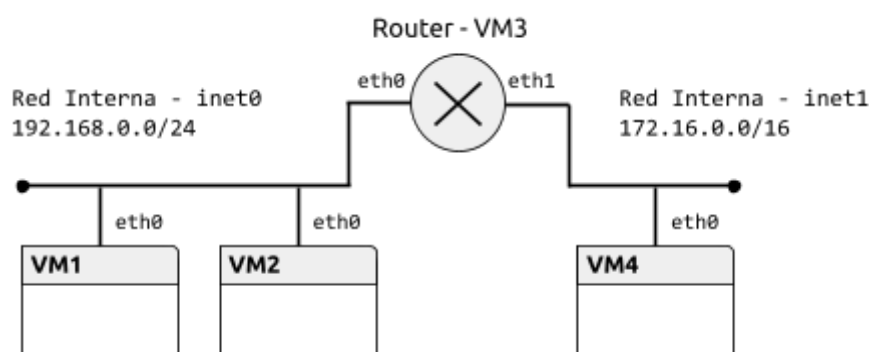
En esta práctica se presentan las herramientas que se utilizarán en la asignatura y se repasan brevemente los aspectos básicos del protocolo IPv4. Además, se analizan las características del protocolo DHCP.

Contenidos

- Preparación del entorno para la práctica
- Configuración estática
- Encaminamiento estático
- Configuración dinámica

Preparación del entorno para la práctica

Configuraremos la topología de red que se muestra en la siguiente figura:



Todos los elementos -el router y las máquinas virtuales VM- son *clones enlazados* de la máquina base ASOR-FE. La configuración de las máquinas se realizará con la utilidad `vtopo1`, que funciona en Linux y Mac (en Windows, la topología ha de crearse directamente con VirtualBox):

1. Definir la máquina base de la asignatura:

```
$ asorregenerate
```

Este comando crea la máquina virtual base (ASOR-FE) en la herramienta VirtualBox.

Nota: El comando `asorregenerate` solo se debe usar en el laboratorio. En otros equipos, descargar el fichero [ASOR-FE.ova](#) e importarlo en VirtualBox.

2. Crear un archivo `pr1.topo1` con la topología de la red, que consta de 4 máquinas y dos redes. El contenido del fichero es:

```
netprefix inet
machine 1 0 0
machine 2 0 0
machine 3 0 0 1 1
machine 4 0 1
```

La sintaxis es:

```
machine <número de VM> <interfaz0> <red0> <interfaz1> <red1> ...
```

3. Crear la topología de red que arrancará las 4 máquinas virtuales (VM1, VM2, Router y VM4).

```
$ vtopol pr1.topol
```

En VirtualBox se definirán las máquinas virtuales asorfemachine_1 (VM1), asorfemachine_2 (VM2), asorfemachine_3 (Router - VM3) y asorfemachine_4 (VM4).

Nota: El comando **vtopol** está instalado en el laboratorio. En otros equipos, descargar el fichero [vtopol](#), darle permisos de ejecución (con `chmod +x`) y copiarlo, por ejemplo, en `/usr/local/bin`.



Activar el portapapeles bidireccional en las máquinas (menú Dispositivos) para copiar la salida de los comandos. Las capturas de pantalla se realizarán usando también Virtualbox (menú Ver).

Las **credenciales de la máquina virtual** son: usuario `cursoresdes`, con contraseña `cursoresdes`.

Configuración estática

En primer lugar, configuraremos cada red de forma estática asignando a cada máquina una dirección IP adecuada.

Ejercicio 1 [VM1]. Determinar los interfaces de red que tiene la máquina y las direcciones IP y MAC que tienen asignadas. Utilizar los comandos `ip address` e `ip link`.

Copiar los comandos utilizados y su salida.

Ip address

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 08:00:27:b8:ad:92 brd ff:ff:ff:ff:ff:ff
```

Ip link

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default
qlen 1000
   link/ether 08:00:27:b8:ad:92 brd ff:ff:ff:ff:ff:ff
```

Ejercicio 2 [VM1, VM2, Router]. Activar los interfaces `eth0` en VM1, VM2 y Router, y asignar una dirección IP adecuada. Utilizar los comandos `ip address` e `ip link`.

En **VM1**:

```
ip address add 192.168.0.1/24 dev eth0
ip link set dev eth0 up
```

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
```

```
link/ether 08:00:27:b8:ad:92 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.1/24 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:feb8:ad92/64 scope link
    valid_lft forever preferred_lft forever
```

En **VM2**:

```
ip address add 192.168.0.2/24 dev eth0
ip link set dev eth0 up
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
```

```
link/ether 08:00:27:ea:9b:f2 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.2/24 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:feea:9bf2/64 scope link
    valid_lft forever preferred_lft forever
```

En **VM3(Router)**:

```
ip address add 192.168.0.3/24 dev eth0
ip link set dev eth0 up
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
```

```
link/ether 08:00:27:9b:e8:c0 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.3/24 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe9b:e8c0/64 scope link
    valid_lft forever preferred_lft forever
```

```
ping -c 1 192.168.0.2
```

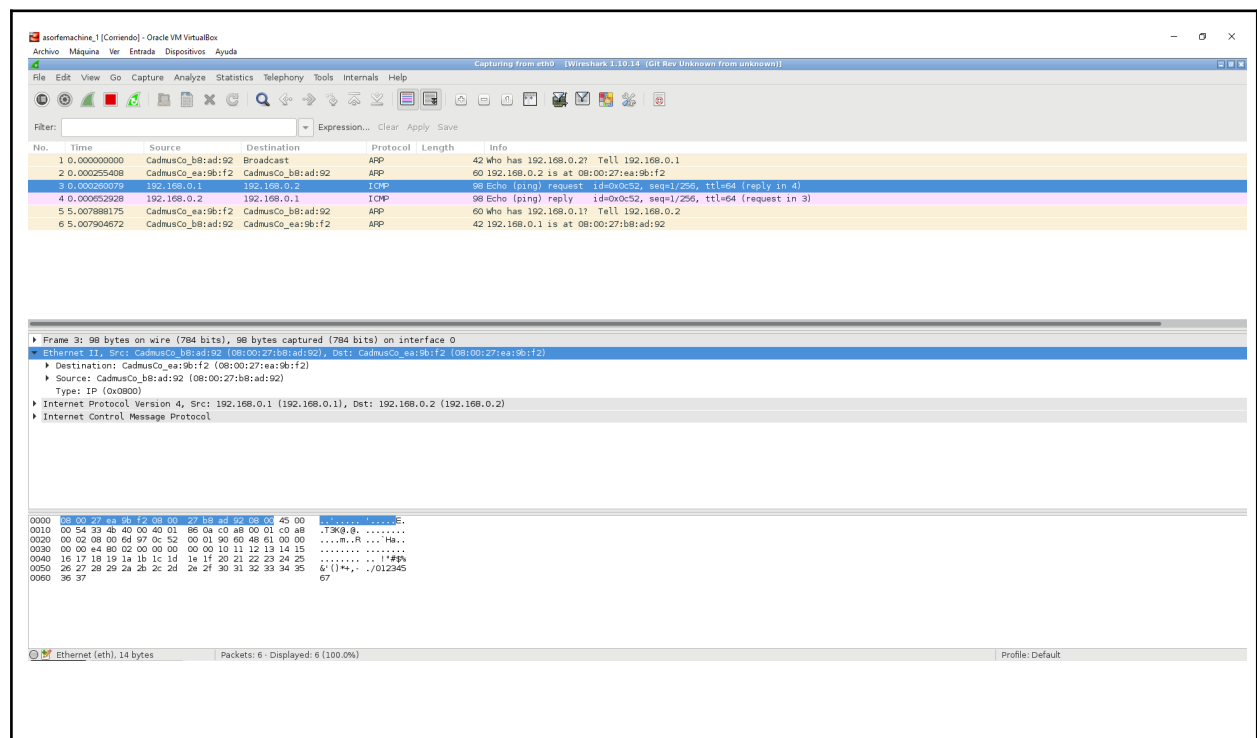
Ejercicio 3 [VM1, VM2]. Abrir la herramienta Wireshark en VM1 e iniciar una captura en el interfaz de red. Desde VM1, comprobar la conectividad con VM2 usando la orden ping. Observar el tráfico generado, especialmente los protocolos encapsulados en cada datagrama y las direcciones origen y destino. Para ver correctamente el tráfico ARP, puede ser necesario eliminar la tabla ARP en VM1 con la orden `ip neigh flush dev eth0`.

Completar la siguiente tabla para todos los mensajes intercambiados hasta la recepción del primer mensaje ICMP Echo Reply:

- Para cada protocolo, anotar las características importantes (p. ej. pregunta/respuesta ARP o tipo ICMP) en el campo "Tipo de mensaje".
- Comparar los datos observados durante la captura con el formato de los mensajes estudiados en clase.

MAC origen	MAC destino	Protocolo	IP origen	IP destino	Tipo de mensaje
------------	-------------	-----------	-----------	------------	-----------------

08:00:27:b8:ad:92	ff:ff:ff:ff:ff:ff	ARP	192.168.0.1	192.168.0.2	Pregunta ARP
08:00:27:ea:9b:f2	08:00:27:b8:ad:92	ARP	192.168.0.2	192.168.0.1	Respuesta ARP
08:00:27:b8:ad:92	08:00:27:ea:9b:f2	ICMP	192.168.0.1	192.168.0.2	Echo request
08:00:27:ea:9b:f2	08:00:27:b8:ad:92	ICMP	192.168.0.2	192.168.0.1	Echo reply



Ejercicio 4 [VM1, VM2]. Ejecutar de nuevo la orden ping entre VM1 y VM2 y, a continuación, comprobar el estado de la tabla ARP en VM1 y VM2 usando el comando `ip neigh`. El significado del estado de cada entrada de la tabla se puede consultar en la página de manual del comando.

Copiar la salida del comando `ip neigh` y describir el estado de cada entrada.

En VM1:

`192.168.0.2 dev eth0 lladdr 08:00:27:ea:9b:f2 STALE`

La máquina virtual 1 conoce que la dirección MAC del host 192.168.0.2 es 08:00:27:ea:9b:f2

En VM2:

`192.168.0.1 dev eth0 lladdr 08:00:27:b8:ad:92 STALE`

La máquina virtual 2 conoce que la dirección MAC del host 192.168.0.1 es 08:00:27:b8:ad:92

El estado STALE significa que el ARP response no llegó en el tiempo esperado

Ejercicio 5 [Router, VM4]. Configurar Router y VM4 y comprobar su conectividad con el comando ping.

Copiar los comandos utilizados y la salida del comando ping.

```
En VM3(Router):
sudo ip address add 172.16.0.1/16 dev eth1
sudo ip link set dev eth1 up

En VM4:
sudo ip address add 172.16.0.2/16 dev eth0
sudo ip link set dev eth0 up

ping -c 1 172.16.0.1

PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=64 time=0.984 ms

--- 172.16.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.984/0.984/0.984/0.000 ms
```

Encaminamiento estático

Según la topología de esta práctica, Router puede encaminar el tráfico entre ambas redes. En esta sección, vamos a configurar el encaminamiento estático, basado en rutas que fijaremos manualmente en todas las máquinas virtuales.

Ejercicio 6 [Router]. Activar el reenvío de paquetes (*forwarding*) en Router para que efectivamente pueda funcionar como encaminador entre las redes. Ejecutar el siguiente comando:

```
$ sudo sysctl net.ipv4.ip_forward=1
```

Ejercicio 7 [VM1, VM2]. Añadir Router como encaminador por defecto para VM1 y VM2. Usar el comando `ip route`.

```
Copiar el comando utilizado.
Tanto en VM1 como en VM2:
sudo ip route add default via 192.168.0.3
```

Ejercicio 8 [VM4]. Aunque la configuración adecuada para la tabla de rutas en redes como las consideradas en esta práctica consiste en añadir una ruta por defecto, es posible incluir rutas para redes concretas. Añadir en VM4 una ruta a la red 192.168.0.0/24 vía Router. Usar el comando `ip route`.

```
Copiar el comando utilizado
en VM4:
sudo ip route add 192.168.0.0/24 via 172.16.0.1

(sudo ip neigh flush dev eth0
ping -c 1 172.16.0.2)
```

Ejercicio 9 [VM1, VM4, Router]. Abrir la herramienta Wireshark en Router e iniciar dos capturas, una en cada interfaz de red. Eliminar la tabla ARP en VM1 y Router. Desde VM1, comprobar la conectividad con

VM4 usando la orden ping. Completar la siguiente tabla para todos los paquetes intercambiados hasta la recepción del primer *Echo Reply*.

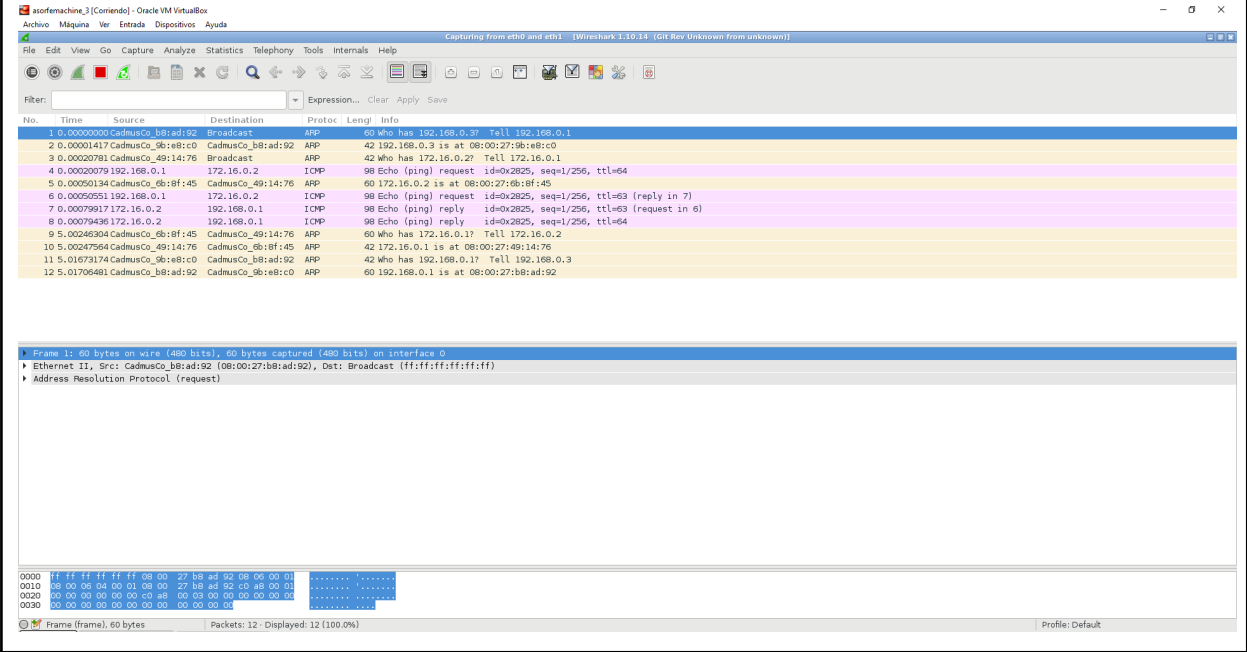
Red 192.168.0.0/24 - Router (eth0)

MAC origen	MAC destino	Protocolo	IP origen	IP destino	Tipo de mensaje
08:00:27:b8:ad:92	ff:ff:ff:ff:ff:ff	ARP	192.168.0.1	192.168.0.3	ARP request
08:00:27:9b:e8:c0	08:00:27:b8:ad:92	ARP	192.168.0.3	192.168.0.1	ARP response
08:00:27:b8:ad:92	08:00:27:9b:e8:c0	ICMP	192.168.0.1	172.16.0.2	Echo request
08:00:27:9b:e8:c0	08:00:27:b8:ad:92	ICMP	172.16.0.2	192.168.0.1	Echo reply

Red 172.16.0.0/16 - Router (eth1)

MAC origen	MAC destino	Protocolo	IP origen	IP destino	Tipo de mensaje
08:00:27:49:14:76	ff:ff:ff:ff:ff:ff	ARP	172.16.0.1	172.16.0.2	ARP request
08:00:27:6b:8f:45	08:00:27:49:14:76	ARP	172.16.0.2	172.16.0.1	ARP response
08:00:27:49:14:76	08:00:27:6b:8f:45	ICMP	192.168.0.1	172.16.0.2	Echo request
08:00:27:6b:8f:45	08:00:27:49:14:76	ICMP	172.16.0.2	192.168.0.1	Echo reply

Copiar dos capturas de pantalla de Wireshark con los mensajes ARP e ICMP.
HE CAPTURADO AMBAS DESDE UNA SOLA PANTALLA



Configuración dinámica

El protocolo DHCP permite configurar dinámicamente los parámetros de red de una máquina. En esta sección configuraremos Router como servidor DHCP para las dos redes. Aunque DHCP puede incluir muchos parámetros de configuración, en esta práctica sólo fijaremos el encaminador por defecto.

Ejercicio 10 [VM1, VM2, VM4]. Eliminar las direcciones IP de los interfaces (`ip addr del`) de todas las máquinas salvo Router.

Ejercicio 11 [Router]. Configurar el servidor DHCP para las dos redes:

- Editar el fichero `/etc/dhcp/dhcpd.conf` y añadir dos secciones `subnet`, una para cada red, que definan, respectivamente, los rangos de direcciones `192.168.0.50-192.168.0.100` y `172.16.0.50-172.16.0.100`. Además, incluir la opción `routers` con la dirección IP de Router en cada red. Ejemplo:

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.50 192.168.0.100;
    option routers 192.168.0.3;
    option broadcast-address 192.168.0.255;
}
subnet 172.16.0.0 netmask 255.255.0.0 {
    range 172.16.0.50 172.16.0.100;
    option routers 172.16.0.1;
    option broadcast-address 172.16.255.255;
}
```

- Arrancar el servicio con el comando `sudo service dhcpd start`.

Ejercicio 12 [Router, VM1]. Iniciar una captura de paquetes en Router. Arrancar el cliente DHCP en VM1 con `dhclient -d eth0` y observar el proceso de configuración. Completar la siguiente tabla:

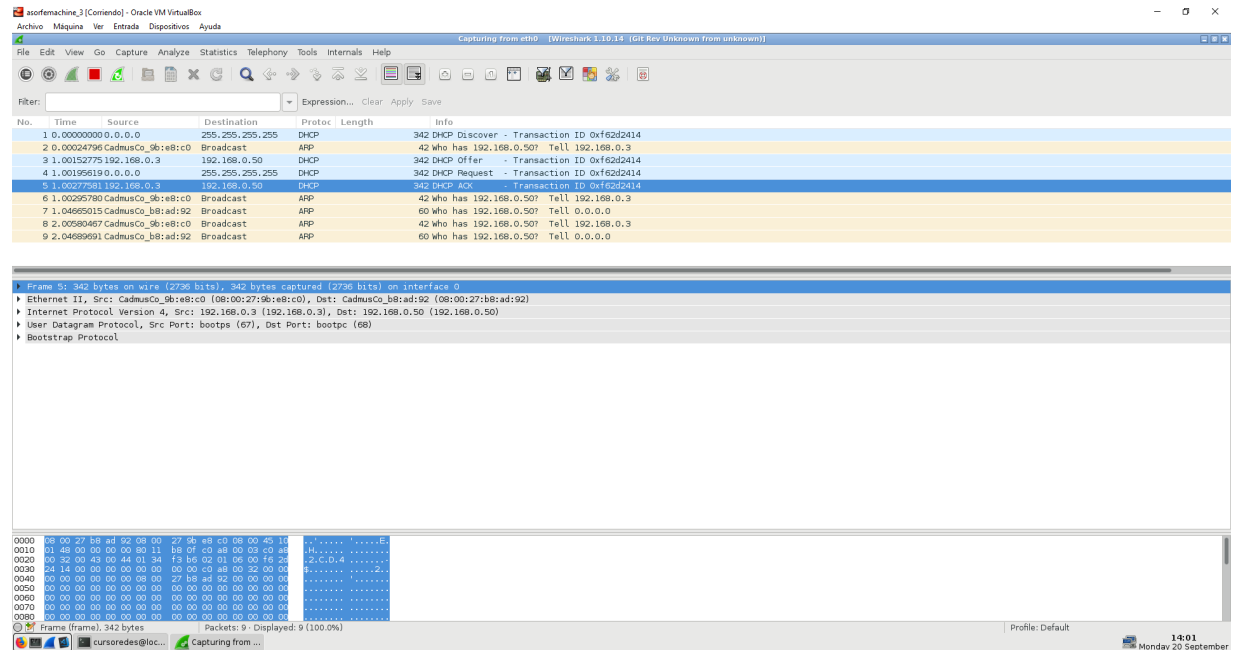
IP Origen	IP Destino	Mensaje DHCP	Opciones DHCP
0.0.0.0	255.255.255.255	DHCP discover	53,50,55,255
192.168.0.3	192.168.0.50	DHCP offer	53,54,51,1,28,3,255
0.0.0.0	255.255.255.255	DHCP request	53,54,50,55,255
192.168.0.3	192.168.0.50	DHCP ack	53(ACK),54,51,1,28,3,255

Copiar la salida del comando `dhclient` y una captura de pantalla de Wireshark con los mensajes DHCP.

Internet Systems Consortium DHCP Client 4.2.5
Copyright 2004-2013 Internet Systems Consortium.
All rights reserved.
For info, please visit <https://www.isc.org/software/dhcp/>

Listening on LPF/eth0/08:00:27:b8:ad:92
Sending on LPF/eth0/08:00:27:b8:ad:92
Sending on Socket/fallback

*DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5 (xid=0x14242df6)
 DHCPREQUEST on eth0 to 255.255.255.255 port 67 (xid=0x14242df6)
 DHCPOFFER from 192.168.0.3
 DHCPACK from 192.168.0.3 (xid=0x14242df6)
 bound to 192.168.0.50 -- renewal in 17526 seconds.*



Ejercicio 13 [VM4]. Durante el arranque del sistema se pueden configurar automáticamente interfaces según la información almacenada en el disco del servidor (configuración persistente). Consultar el fichero `/etc/sysconfig/network-scripts/ifcfg-eth0` de VM4, que configura automáticamente `eth0` usando DHCP. Para configuración estática, se usarían las siguientes opciones:

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=<dirección IP estática>
PREFIX=<tamaño del prefijo de red>
GATEWAY=<dirección IP estática del encaminador por defecto (si existe)>
DEVICE=eth0
```

En VM4 aparece:

```
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
NAME=eth0
DEVICE=eth0
ONBOOT=no
```

Nota: Estas opciones se describen en detalle en `/usr/share/doc/initscripts-*/sysconfig.txt`.

Ejercicio 14 [VM2, VM4]. Comprobar la configuración persistente con DHCP usando órdenes `ifup` e

Mostramos las conexión mediante ifup de VM2 y VM4 y después el ping de VM4 a VM2

exportmachine_3 [Cordex] - Oracle VM VirtualBox

ArchiveMáquinaVer EntendaDispositivosAjuda

Capturing from eth0 and eth1 [Wireshark 3.10.14 (Git Rev Unknown from unknown)]

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter:Expression...ClearApplySave

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000:::		ff02::1:ffeb:bfa5	ICMPv6	78	Neighbor Solicitation for fe80:a00:27ff:febb:bfa5
2	0.0009884s:::		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
3	0.0046490s 0.0.0.0		255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x644030c
4	0.0056470 172.16.0.1		172.16.0.50	DHCP	342	DHCP ACK - Transaction ID 0x644030c
5	0.0074147 CadmusCo_6b:bfa5	Broadcast	APP	60	Who has 172.16.0.50? Tell 0.0.0.0	
6	0.4429507:::		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
7	0.9995193 fe80:a00:27ff:febb:ff02::16		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
8	1.0779697 CadmusCo_6b:bfa5	Broadcast	APP	60	Who has 172.16.0.50? Tell 0.0.0.0	
9	1.1610207 fe80:a00:27ff:febb:ff02::16		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
10	4.00227994:::		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
11	4.1124965s 0.0.0.0		255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x580e8c2
12	4.1130391 192.168.0.3		192.168.0.51	DHCP	342	DHCP ACK - Transaction ID 0x580e8c2
13	4.1452445 CadmusCo_ea:9bf2	Broadcast	APP	60	Who has 192.168.0.51? Tell 0.0.0.0	
14	4.7606218:::		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
15	4.7803574s:::		ff02::1:ffea:9bf2	ICMPv6	78	Neighbor Solicitation for fe80:a00:27ff:feaa:9bf2
16	5.1456073 CadmusCo_ea:9bf2	Broadcast	APP	60	Who has 192.168.0.51? Tell 0.0.0.0	
17	5.7827562 fe80:a00:27ff:feaa:ff02::16		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
18	6.18692474 fe80:a00:27ff:feaa:ff02::16		ff02::16	ICMPv6	90	Multicast Listener Report Message v2
19	10.907277 CadmusCo_6b:bfa5	Broadcast	APP	60	Who has 172.16.0.1? Tell 172.16.0.50	
20	10.9072482 CadmusCo_49:1476	CadmusCo_6b:bfa5	APP	42	172.16.0.1 is at 08:00:27:49:14:76	
21	10.9074178 CadmusCo_9b:e8:c0	Broadcast	APP	42	Who has 192.168.0.51? Tell 192.168.0.3	
22	10.9074081 172.16.0.50	192.168.0.51	ICMP	98	Echo (ping) request id=0xc276, seq=1/256, ttl=64	
23	10.9076145 CadmusCo_ea:9bf2	CadmusCo_9b:e8:c0	APP	60	192.168.0.51 is at 08:00:27:ae:9b:f2	
24	10.9076262 172.16.0.50	192.168.0.51	ICMP	98	Echo (ping) reply id=0xc276, seq=256, ttl=63 (reply in 25)	
25	10.9077749 192.168.0.51	172.16.0.50	ICMP	98	Echo (ping) reply id=0xc276, seq=256, ttl=64 (request in 24)	
26	10.9077792 192.168.0.51	172.16.0.50	ICMP	98	Echo (ping) reply id=0xc276, seq=256, ttl=63	
27	15.9182903 CadmusCo_9b:e8:c0	CadmusCo_ea:9bf2	APP	60	Who has 192.168.0.3? Tell 192.168.0.51	
28	15.9183069 CadmusCo_9b:e8:c0	CadmusCo_ea:9bf2	APP	42	192.168.0.3 is at 08:00:27:9b:e8:c0	
29	15.9213006 CadmusCo_49:1476	CadmusCo_6b:bfa5	APP	42	Who has 172.16.0.50? Tell 172.16.0.1	
30	15.9222439 CadmusCo_6b:bfa5	CadmusCo_49:1476	APP	60	172.16.0.50 is at 08:00:27:6b:bfa5	

Frame 9: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 1

Ethernet II, Src: CadmusCo_6b:bfa5 (08:00:27:6b:bfa5), Dst: Ipv6cast::00:00:00:16 (33:33:00:00:00:16)

Internet Protocol Version 6, Src: fe80:a00:27ff:febb:bfa5 (fe80:a00:27ff:febb:bfa5), Dst: ff02::16 (ff02::16)

0010 33 33 00 00 01 16 08 00 27 6b bf a5 b8 dd 0a 00 33.....k.E..
0020 00 00 00 24 00 01 f8 80 00 00 00 00 00 00 00 00f.....
0030 27 ff f1 f6 bf a5 ff 02 00 00 00 00 00 00 00 00k.E.....
0040 00 00 00 00 00 16 3a 00 05 02 00 09 01 00 8f 00:.....
0050 21 a8 00 00 01 04 00 00 00 ff 02 00 00 00 00 00!.....

eth0 and eth1 <-live capture in progress. Packets 30 / Displayed: 30 (100%)

Profile: Default

Monday 30 September 14:35

```
[cursoredes@localhost ~]$ sudo ifup eth0
Determining IP information for eth0... done.
[cursoredes@localhost ~]$ ping -c 1 192.168.0.51
PING 192.168.0.51 (192.168.0.51) 56(84) bytes of data:
64 bytes from 192.168.0.51: icmp_seq=1 ttl=63 time=0.740 ms

--- 192.168.0.51 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.740/0.740/0.740/0.000 ms
[cursoredes@localhost ~]$
```